Das Darknet

Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus“ der Kriminellen?

Von Dr. Sabine Vogt, Wiesbaden1

1 Einführung

... November 2015: Shiny-Flakes, 20-jähriger Rauschgifthändler aus Leipzig verkaufte aus der elterlichen Wohnung Betäubungsmittel im großen Stil über das Internet ...
... Januar 2016: Waffenhändler Max Mustermann, 26-jähriger Mechatronik-Student aus Unterfranken, finanzierte sich mit dem illegalen Waffenhandel sein Studium und seine Waffenleidenschaft ...
... Juni 2016: 32-jähriger Optiker und Sportschütze aus Heidelberg, Nickname Dosensuppe, verbesserte mit dem gewerbsmäßigen illegalen Waffenhandel seinen Lebensunterhalt ...

Schlagzeilen wie diese haben das Darknet in das Bewusstsein der Öffentlichkeit gerückt.
Der Amoklauf am Münchener Olympia-Einkaufszentrum am 22. Juli 2016, bei dem der 18-jährige Schütze mit einer über das Darknet-Forum „Deutschland im Deep Web“ erworbenen Pistole Glock 17 neun Menschen und dann sich selbst erschoss, hat überdies aufgezeigt, welches Gefahrenpotenzial mit diesem Phänomen verbunden ist.

2 Was ist das Darknet und wo findet es sich?

2.1 Clearnet und Deepweb2

Beim Internet wird zwischen verschiedenen Bereichen unterschieden.
Das **Clearnet** (auch Visible Web, Surface Web, Open Web u.a.) ist das weitläufig bekannte Internet, welches mit normalen Browserprogrammen (Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome etc.) bedienbar und durch Suchmaschinen wie Google, bing etc. einfach und intuitiv zu handhaben ist. Bereits im Clearnet sind vielfältige illegale Inhalte vorhanden. Auf verschiedenen Plattformen werden sowohl Güter als auch Dienstleistungen aus den Bereichen Cybercrime im engeren Sinn**3** sowie „klassischen“ Phänomenen wie etwa dem Handel mit Betäubungsmitteln, Waffen, Falschgeld etc. angeboten.

Das **Deepweb** (auch Hidden Web, Invisible Web) ist jener Teil des Internet, der nicht durch die allgemeinen Suchmaschinen auffindbar ist. Inhalte des Deepweb können beispielsweise Datenbanken, Intranets oder Fachwebseiten sein, die zwar regelmäßig mittels normalen Browserprogrammen erreicht werden können, nicht jedoch in gängigen Suchmaschinen verlinkt und daher hierüber nicht auffindbar sind. Inhalte des Deepweb sind regelmäßig in geschützten Bereichen oder in eigenen Netzwerken abgelegt, so dass seine Inhalte nur mit einer Zugriffsberechtigung aufgerufen werden können. Auch private Teile des sozialen Netzwerks Facebook zählen zum Deepweb.
Weiterhin gibt es Netzwerke, die nur über spezielle Software erreichbar sind und sich durch eine besonders starke Verschlüsselung und/oder Anonymisierung auszeichnen. Das sog. **Darknet** umfasst Wikis/Blogs mit unterschiedlichen – auch legalen – Zielrichtungen sowie kriminelle/inkriminierte Kommunikations- und Handelsplattformen. Wie in der realen Welt gibt es berechtigte Gründe, warum eine Information wie z.B. die Identität eines Nutzers nicht publik gemacht werden soll. Hierzu zählt beispielsweise der Schutz der Presse- und Meinungsfreiheit. Kriminelle missbrauchen diese Anonymität zur Begehung von Straftaten. Die Funktionsweise verschiedener Software zur Nutzung des Darknet (z.B. Tor-Browser-Bundle, Invisible Internet Project [I2P], Freenet) bietet dem Anwender eine umfangreiche und leicht zugängliche Anonymität, weshalb das Darknet einen attraktiven Raum für Straftäter darstellt. Sie sorgt für ein hohes Sicherheitsgefühl auf Seiten der Kriminellen.
Im Visible Web sind diverse Hinweise und Informationen zu Plattformen im Darknet zu finden. Beispielsweise gibt die Webseite *DeepDotWeb***4** eine Übersicht über bekannte Plattformen im Tor-Netzwerk inklusive Angaben zur Online-Zeit, Registrierungsumständen, Kommission, Bewertung, sowie der URL, über die sie zu erreichen sind.
Einen bedeutenden Teil des Darknet machen die Darknet-Markets aus, also kriminelle Marktplätze, bei denen inkriminierte Güter anonym gehandelt werden. Diese decken die Bedürfnisse der „Erlangungskriminalität“ (Betäubungsmittel, Waffen, Arzneimittel, Falschgeld, Kinderpornografie, gefälschte Dokumente etc.) ab und bieten zunehmend unter dem Schlagwort „Crime-as-a-Service“ kriminelle Dienstleistungen und Software an.

2.2 Darknet – Funktion

Zur Nutzung des Darknet wird überwiegend der Tor-Browser verwendet. TOR war ursprünglich ein Akronym für „The Onion Routing“ oder „The Onion Router“ (engl. *Onion* = Zwiebel). Das aktuelle Projekt „The Tor Project“ ist als gemeinnützige Organisation eingestuft und widmet sich der Forschung, der Entwicklung und der Schulung zum Thema Internetanonymität und Datenschutz.
Die Kommunikation zwischen Client und *hidden service* läuft immer über mehrere Server im Tor-Netzwerk. Der Client handelt mit dem *hidden service* einen sog. Rendezvous-Punkt (auf einem Tor-Server) aus, an dem sich die beiden Gegenstellen treffen. Die jeweiligen Routen des Datenverkehrs von Client bzw. *hidden service* zum Rendezvous-Punkt werden durch den Durchlauf mehrerer Tor-Knoten so stark verschleiert, dass eine Verfolgung dieses Datenverkehrs nicht möglich ist und somit auch kein Rückschluss auf den Datenursprung gezogen werden kann.**5**
Anders als im Clearnet gibt es im Tor-Netzwerk zudem keine Möglichkeit, eine Domain zu einer IP-Adresse aufzulösen. Zu einer Onion-Domain gibt es auch keine Dienste, die weitere Infos über diese Domain ausgeben (Whois-Server).
Insgesamt nutzen nach eigenen Angaben des Tor-Projekts durchschnittlich zwei Millionen Menschen täglich den Tor-Browser. Davon kommen 10 Prozent (200.000) aus Deutschland.**6**

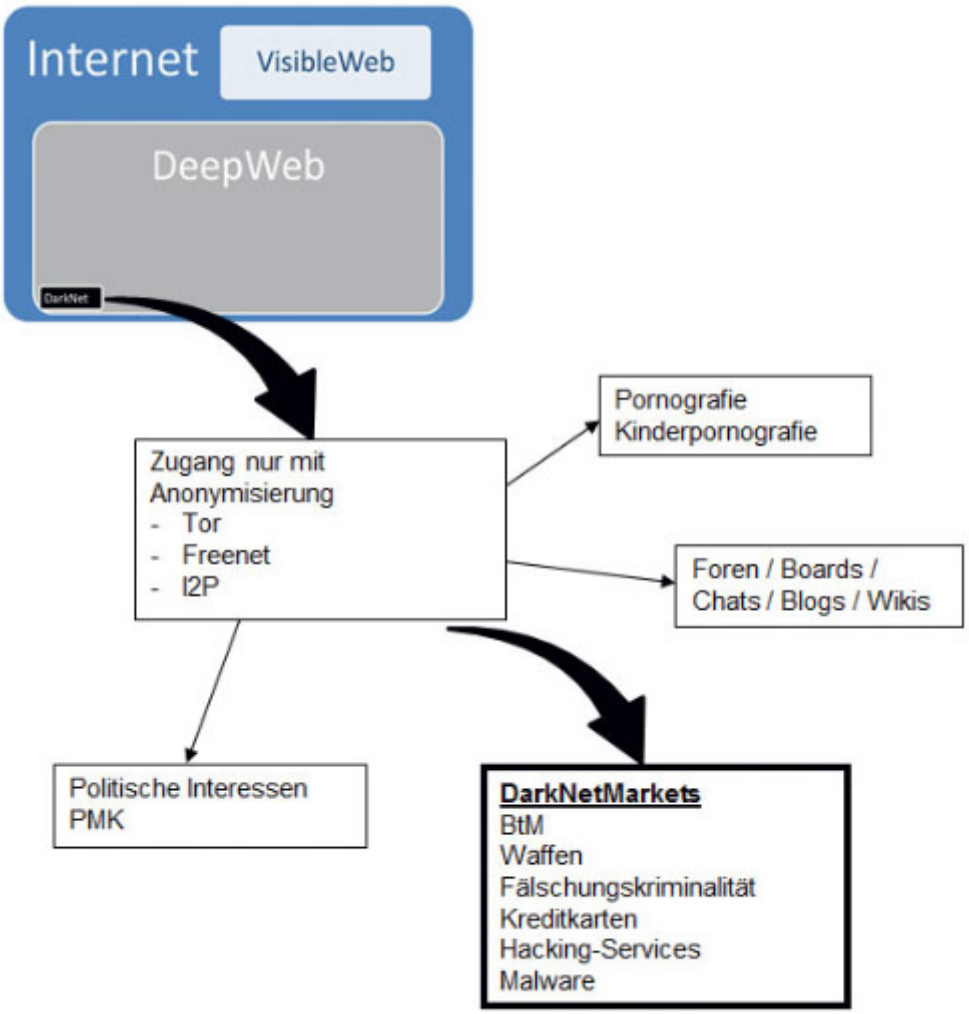
2.3 Darknet – Aufbau

Im Oktober 2013 verkündete das FBI die Sicherstellung des Darknet-Forums Silk Road, sowie die Festnahme seines Betreibers. Silk Road war bis dahin der größte Drogenumschlagplatz im Netz. Darüber hinaus waren Angebote aus den Bereichen Fälschungs- und Geldwäschekriminalität umfasst. Laut FBI wurde über Silk Road ein Umsatz von über 1,2 Milliarden US-Dollar**7** (monatlich zwei Millionen**8** US-Dollar) generiert.
Silk Road ist nur ein Beispiel für einen kriminellen Online-Marktplatz im Darknet. Je nach Markt werden Betäubungsmittel,

Arzneimittel, Waffen, Falschgeld, Dokumente, elektronische Daten, Software sowie Kinder- und Jugendpornografie u.v.m. zum Kauf angeboten. Die Zahlungen werden über sog. Krypto-Währungen wie Bitcoin (BTC) geleistet, wobei teilweise durch die Marktplatzbetreiber ein Treuhandservice angeboten wird (sog. Escrow).
Die Angebote und Kommunikation über die Marktplätze und Foren werden überwiegend in englischer Sprache verfasst, in vielen Plattformen lässt sich jedoch ein Bezug nach Deutschland feststellen (z.B. Versand aus Deutschland, Anfragen in deutscher Sprache). Aktuell geht das BKA von etwa 50 Plattformen (Marktplätze und Foren) mit Deutschlandbezug aus.
Es wird unterschieden zwischen Marktplätzen mit oder ohne begleitendes Forum, jenen mit besonderen Zugangsberechtigungen und solchen, die zum Erhebungszeitraum nicht erreichbar waren. Etwa 20 Marktplätze weisen eine operative Bedeutung für das BKA aus.
DreamMarket ist ein Beispiel der Plattformen mit begleitendem Forum. Der Marktplatz weist ca. 55.000 Kaufangebote auf und verzeichnet ca. 20.000 Nutzer. *Alphabay***9** listete im Zeitraum Juni/Juli 2016 ca. 66.000 Kaufangebote bei einer Nutzerzahl von über 75.000. Betäubungsmittel machen hierbei den größten Anteil an Kaufangeboten aus (ca. 52.000), darüber hinaus werden unter anderem Waffen (ca. 500), Falschgeld (ca. 300), Daten und Arzneimittel angeboten. Ca. 3.500 der Betäubungsmittel-Angebote und ca. 90 der Waffen-Angebote scheinen aus Deutschland zu kommen.
In *Deutschland im Deep Web* werden Betäubungsmittel, Arzneimittel, Falschgeld und Waffen gehandelt. Darüber hinaus gibt es verschiedene Themenbereiche wie Religionen, Sport, Politik und Wirtschaft, in welchen die Mitglieder diskutieren.
Bei der Anzahl der Plattformen ist ein leichter Rückgang festzustellen. Daraus ist jedoch kein Rückgang der Benutzerzahlen oder Angebote abzuleiten. Möglich ist, dass sich Nutzer, beispielsweise in Folge einer Abschaltung einer etablierten Plattform, temporär auf bestimmte andere Plattformen konzentrieren.**10**

Die Landschaft der kriminellen/inkriminierten Kommunikations- und Handelsplattformen unterliegt grundsätzlich einer großen Dynamik und Fluktuation. Eine Lagedarstellung kann demnach nur eine Momentaufnahme darstellen.
Der mehr als rege Handel mit illegalen oder inkriminierten Gütern im Darknet hat innerhalb der letzten Jahre eine enorme Entwicklung durchlaufen. Mittlerweile hat sich eine globale Industrie entwickelt, die nahezu keinen Kundenwunsch offen lässt. Marktplätze übernehmen dabei bekannte Strukturen von legalen Plattformen wie ebay und Amazon, die Produkte werden mit Fotos und Beschreibungen aufgelistet, die Community diskutiert sehr intensiv über die Vertrauenswürdigkeit von Händlern**11** und es gibt einen 24/7-Kundensupport. „Crime-as-a-Service“-Angebote haben sich sowohl im Deepweb als auch im Darknet als feste Komponenten in Angebots- und Produktpaletten etabliert. Hierbei werden Dienstleistungen zur Verfügung gestellt, die die Durchführung jeder Art von Cybercrime ermöglichen bzw. erleichtern. Dies gestattet interessierten Kriminellen ohne technische Vorkenntnisse und mit vergleichsweise geringem Aufwand Zugang zu hochentwickelten Cyber-Werkzeugen und macht damit das Darknet zu einem Einkaufszentrum für jedermann.Der bereitgestellte Support umfasst beispielsweise Updates für Schadsoftware, Beratungsdienste, Anti-Erkennungsmechanismen sowie die Hilfestellung bei technischen Problemen.

Weiterhin werden „Infection on Demand“ (Verteilung von Schadsoftware auf Anforderung/Abruf) sowie Test-Portale angeboten. Hier können die von den Tätern erworbenen oder selbst programmierten Schadsoftware-Varianten auf Detektierbarkeit durch aktuelle Cyber-Sicherheitsprodukte wie z.B. Antivirenprogramme getestet werden, um durch Anpassungen die Erfolgsaussichten für eine „Verteileroffensive“ zu verbessern.
Besonders attraktiv in der Produktpalette zu Cybercrime-as-a-Service ist die Mitgestaltungskomponente. Im Jahr 2015 wurde ein „digitaler Erpressungsdienst“ festgestellt, der über das Tor-Netzwerk erreichbar ist. Dieser ermöglicht eine kostenlose und mit geringem Aufwand verbundene individuelle Zusammenstellung von Malware (sog. Toolkits). Die Anbieter des Dienstes erhalten bei einer erfolgreichen Lösegeldzahlung eine Umsatzbeteiligung, wobei die Lösegeldzahlung in der Regel in Form von Bitcoin über den Schadsoftwareanbieter selbst abgewickelt wird. Über eine vom Schadsoftwareanbieter zur Verfügung gestellte Kontrollplattform kann der Nutzer des Toolkits die von ihm hervorgerufenen Infektionen einsehen und seinen verbliebenen Anteil an den Lösegeldern an sich selbst auszahlen. Für die Verbreitung der Schadsoftware werden ebenfalls Dienstleistungen angeboten. Auch hier kann der Kunde selbst bestimmen, wen die Schadsoftware angreifen soll.



2.4 Illegale Inhalte des Darknet

Im Darknet findet sich die komplette Bandbreite krimineller Aktivitäten wieder, bei denen das Internet als Tatmittel nutzbar ist oder auch Cybercrime im engeren Sinne vorliegt (wobei sich letzteres Phänomen dominanter im Bereich der Underground Economy zeigt). Grundsätzlich sind daher alle Delikte im Darknet anzutreffen.
Viele Plattformen im Darknet sind nach den jeweiligen illegalen Angeboten übersichtlich aufgebaut, aus Gründen der Abschottung und Konspiration oft streng hierarchisch gegliedert und werden professionell betrieben. Die Gewinnerzielung steht dabei im Vordergrund – das anonyme Handeln wird dabei durch die Verwendung digitaler Zahlungsmittel (Krypto-Währungen wie „Bitcoins“ u.a.) ermöglicht. Hingegen geht es z.B. bei Plattformen, auf denen pädosexuelle Nutzer aktiv sind, um das Tauschen kinderpornografischer Inhalte oder im Bereich politisch motivierter Kriminalität um den Informationsaustausch mit Gleichgesinnten.

3 Darknet und Strafverfolgung

Die Entwickler von Anonymisierungssoftware wie Tor sind bestrebt, eine Identifizierung der Nutzer grundsätzlich unmöglich zu machen. Herkömmliche Ermittlungsansätze wie IP-Adressen, Domainnamen oder verifizierte Nutzerdaten stehen daher regelmäßig nicht zur Verfügung. Der Einsatz von Krypto-Währungen erschwert die Rückverfolgung von Geldströmen zusätzlich. Hinzu kommt ein vielfach vorhandener hoher Grad an Konspiration innerhalb der Szene. Zudem: Kriminalität im digitalen Raum spielt sich unabhängig vom nationalen Recht und Zuständigkeiten ab.
Gleichzeitig findet sich im Internet eine Flut von Daten und Informationen, die z.T. auch allgemein zugänglich sind und von Relevanz für Ermittlungen sein können. Insofern sind hier die klassischen zwei Seiten einer Medaille gegeben: Einerseits bestehen Ermittlungsansätze, andererseits sind die Strafverfolgungsbehörden mit „big data“ und deren Auswertung und Analyse konfrontiert.
Trotz dieser Herausforderungen gelingen dem BKA und den Polizeibehörden der Länder sowie dem Zoll immer wieder Erfolge bei der Identifizierung und Verfolgung von Straftätern im digitalen Raum – und im Darknet. Dieser Erfolg beruht auf einer Vielzahl von Faktoren:

- Kombination von innovativen, technisch gestützten analytischen Methoden mit „klassischen“ polizeilichen Vorgehensweisen
- Durchführung „digitaler“ Finanzermittlungen
- Gemeinsam abgestimmte und auch durchgeführte „Operationen“ auf nationaler Ebene unter Einbeziehung der Staatsanwaltschaften
- Intensive Zusammenarbeit auf europäischer Ebene – unter Nutzung von Europol, Interpol und im internationalen Kontext
- Gute technische Ausstattung der Cyber- und Forensikdienststellen
- Einsatz von qualifiziertem Personal und IT-Experten
- Veränderte Personalgewinnung und „clevere“ Qualifizierung.

Bundesweit haben sich in den letzten Jahren Cyberdienststellen in der Polizei und beim Zoll entwickelt, die Cybercrime und speziell Kriminalität im Darknet bekämpfen. Hier werden Experten eingesetzt, die sowohl über eine IT- Expertise verfügen als auch über kriminalpolizeiliches know how. Das BKA praktiziert derzeit eine sog. „Tandemlösung“, d.h., dass ein Cyberanalyst (IT-Experte) zusammen mit einem Polizeibeamten gemeinsam am Fall arbeitet. Andere Bundesländer verfolgen andere Modelle, wie z.B. den Einsatz von „Cybercops“; dabei handelt es sich um IT-Experten, die in einer verkürzten Ausbildung an die Aufgaben eines Kriminalbeamten herangeführt werden. Auch bei den Staatsanwaltschaften werden spezialisierte Dienststellen neu eingerichtet oder erweitert, die sich ausschließlich auf die Bekämpfung von Cybercrime bzw. der Kriminalität im Kontext Internet konzentrieren.
„Erfolge“, die diese Spezialisten bei der Bekämpfung von Kriminalität im Darknet erzielen, fußen oftmals auf einer Kombination von verschiedenen Auswerte- und Ermittlungsansätzen. Die Analyse der Massendaten, die im Internet und auch im Darknet „produziert“ werden, kann ohne IT nicht erfolgen – hier sind an den jeweiligen Fall angepasste „Werkzeuge“ erforderlich. Zudem sind verdeckte Ermittlungen oft ein entscheidender Faktor, um letztlich die Täter zu identifizieren.
Zudem hat sich gezeigt, dass in gemeinsamen polizeilichen Bund-Länder „Operationen“ gute Erfolge erreichbar sind. Hier können die Ziele einer gemeinsamen Auswertung oder Ermittlung abgestimmt, die Vorgehensweise vereinbart und die personellen sowie technischen Möglichkeiten der beteiligten Dienststellen berücksichtigt werden. Positive Erfahrungen in der Praxis liegen bereits vor.
Digitale Kriminalität kann nur erfolgreich durch internationale Zusammenarbeit bekämpft werden – viele gemeinsame polizeiliche Operationen werden daher heute mit Hilfe von Europol koordiniert und durchgeführt. Hier nutzen europäische Staaten das sog. EC 3 – eine eigens bei Europol eingerichtete Arbeitsplattform. Das BKA hat für diese Arbeit einen Verbindungsbeamten zu Europol entsandt. Gemeinsame Projekte und Operationen werden zudem im Rahmen des sog. EU-Policy Cycle unter Nutzung der europäischen Förder-Finanzhilfen durchgeführt, so dass ein direkter operativer Nutzen entsteht. International besteht zudem ein enger Arbeitsverbund über das G 7 Netzwerk; ferner sind Arbeitsverbünde bi- und multilateraler Art mit Polizeien anderer Staaten weltweit entstanden. Auch Interpol hat in Singapur das Global Complex for Innovation eingerichtet, ein Zentrum, welches die Cyberkriminalität von dort aus ins Visier nimmt. – Das Netzwerk internationaler Kooperation unter den Polizeien ist eng gespannt!
Ferner bedarf es auch eines permanenten erheblichen „Investments“ in die technische Ausstattung, die Personalgewinnung sowie die Aus- und Fortbildung von Kriminalbeamten und IT-Experten – dies sind dauerhafte Kostenfaktoren, gerade wenn man an die Schnelllebigkeit der Entwicklungen im IT-Bereich denkt. Zudem sind auch „Bündnisse“ mit Universitäten und Instituten zu schließen, um den Entwicklungs- aber auch den Fortbildungsbedarf zu decken. Das bedeutet: eine erfolgreiche Bekämpfung von Cybercrime im „Niedrigpreissegment“ hat wenig Aussicht auf Erfolg!
Weiterer Handlungsbedarf besteht im Bereich der Rechtsfortentwicklung – wie z.B. bei der Frage, ob nicht das kriminelle Handeln von Administratoren und Moderatoren auf illegalen Plattformen einer eigenen Strafbarkeit unterworfen werden sollte. Die Bereitstellung einer technischen Infrastruktur für kriminelle Zwecke ermöglicht nicht nur eine Tatbegehung durch Dritte sondern bildet auch den Tatort und stellt das technische Tatwerkzeug zur Verfügung.

Europäisches Recht wie z.B. die Budapester Cybercrime Convention bedarf der weiteren Umsetzung. Letztlich muss es gelingen, die Strafverfolgung im digitalen Raum über die Ländergrenzen hinweg zu gewährleisten und hier die rechtlichen Instrumente anzupassen.
Die hier angedeuteten Herausforderungen werden sich auch in Zukunft weiter dynamisieren. Veränderungen, Innovationen, wie z.B. die Blockchain-Technologie im Bereich der Kryptowährungen, geben den Takt vor und haben unmittelbare Auswirkungen auf die Arbeit der Strafverfolgungsbehörden. Dies stellt oft völlig neue Anforderungen an uns als Strafverfolgungsbehörden, auf die wir uns einstellen müssen.
Dennoch – die Nachricht für die Täter im digitalen Raum muss lauten: Es gibt auch dort keine rechtsfreien Räume.

Anmerkungen

1. Frau Dr. Sabine Vogt leitet die Abteilung Schwere und Organisierte Kriminalität des Bundeskriminalamtes.
2. Die Begriffe und erklärten Sektoren des Internet stellen keine abschließenden Definitionen dar. Für das BKA und andere Polizeibehörden ist jedoch eine Festlegung bedeutsam, um eine Grundlage für eine möglichst einheitliche Sprachregelung zu schaffen.
3. Cybercrime im engeren Sinn umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (z.B. Durchführung von Distributed Denial of Service [DDoS]-Angriffen, Hacking, etc.).
4. www.deepdotweb.com.
5. Detaillierte Beschreibung der Funktion des Tor-Browsers findet sich in der Broschüre „Tor-Netzwerk“ des BKA, aufzurufen unter www.extrapol.de.
6. metrics.torproject.org.
7. www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html.
8. www.zeit.de/digital/internet/2015-05/ross-ulbricht-silk-road-strafmass-urteil.
9. Nähere Informationen finden sich in der Broschüre „Tor-Netzwerk“ des BKA, aufzurufen unter www.extrapol.de.
10. Die Abschaltung einer Plattform führt gemäß einer Studie der Carnegie Mellon Universität in Pittsburgh gerade nicht zu einem Einbruch des Handelsgeschehens sondern zur Verlagerung auf andere Plattformen (Quelle: Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, Kyle Soska and Nicolas Christin, Carnegie Mellon University, 2015).
11. Marktplatz des Verbotenen, Handelsblatt, 5.8.2016.